UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WISCONSIN

SCOTT LINMAN, on behalf of himself and all others similarly situated, Plaintiff, v. **MARTEN TRANSPORT, LTD.,** Defendant.	**Case No.** **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff Scott Linman, ("Plaintiff") brings this Class Action Complaint against Defendant Marten Transport, Ltd. ("Defendant" or "Marten"), individually and on behalf of all others similarly situated ("Class Members"), and alleges, upon personal knowledge as to his own actions and his counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard personally identifiable information that Defendant required from job applicants as a condition of potential employment, including but not limited to names and Social Security numbers (collectively, "personally identifiable information" or "PII").

2. Defendant also failed to provide timely, accurate, and adequate notice to Plaintiff and Class Members that their PII had been exposed. Defendant failed to inform Plaintiff and Class Members of precisely what types of personally identifiable information was unencrypted and now in the possession of unknown third parties.

3. Defendant is a publicly traded freight carrier and logistics company with a

market capitalization exceeding one billion dollars. It operates a fleet of more than 3,000 refrigerated trucks and has thousands of employees.

4. Defendant's prospective employees, current employees, and former employees entrust them with an extensive amount of their PII. Without explanation or disclosure, Defendant retains this information – even after any employment relationship with Defendant ends, or in the case of prospective employees, even if they are not hired to work for Defendant.

5. From September 30, 2021 to October 4, 2021, this PII was continuously exposed by Defendant and accessed by cybercriminals due to the way Defendant stored and maintained PII on its systems (the "Data Breach").

6. In March 2022, Defendant confirmed the PII of approximately 35,294 individuals was exposed in the Data Breach.[1]

7. Defendant waited until late March 2022 to notify many victims of the Data Breach. It was also around this time that Defendant began notifying various states Attorneys General of the Data Breach. For example, on March 25, 2022, Defendant notified the attorneys general of California, Maine, Montana, Vermont, and Washington.[2] The

[1] https://apps.web.maine.gov/online/aeviewer/ME/40/386f1029-e915-49dc-bdb6-426bfea19ba2.shtml (last visited April 5, 2022).
[2] https://oag.ca.gov/privacy/databreach/list (last visited April 5, 2022); https://apps.web.maine.gov/online/aeviewer/ME/40/386f1029-e915-49dc-bdb6-426bfea19ba2.shtml (last visited April 5, 2022); https://dojmt.gov/consumer/databreach/# (last visited April 5, 2022); https://ago.vermont.gov/blog/2022/03/25/marten-transport-data-breach-notice-to-consumers/ (last visited April 5, 2022); https://www.atg.wa.gov/data-breach-notifications (last visited April 5, 2022).

submission of notification to the California Attorney General is particularly notable because it indicates that the PII involved in the Data Breach was unencrypted on Defendant's system when accessed by the cybercriminals.[3]

8. By obtaining, collecting, storing, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendant admits that the unencrypted PII exposed in the Data Breach included names and Social Security numbers.

9. The exposed PII of Plaintiff and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII to other criminals. Plaintiff and Class Members now face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers. Plaintiff and Class Members have already experienced and will continue to experience various instances of fraud, as detailed herein, for years to come.

10. This PII was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the PII of Plaintiff and Class Members. In addition to Defendant's failure to prevent the Data Breach, after discovering the breach, Defendant failed to timely report it to the states' Attorneys General and affected Class Members. Defendant has also purposefully maintained secret the specific vulnerabilities and root

[3] California law requires companies to notify California residents "whose ***unencrypted*** personal information was, or is reasonably believed to have been, acquired by an unauthorized person" due to a "breach of the security system[.] Cal. Civ. Code §1798.82(a)(1) (emphasis added).

causes of the Data Breach and has not informed Plaintiff and Class Members of that information.

11. As a result of Defendant's delayed notification, Plaintiff and Class Members had no idea their PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

12. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

13. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, mitigation, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and (iv) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain in Defendant's possession and is therefore subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

14. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that their PII was safeguarded. Defendant failed to take available steps to prevent the Data Breach and accompanying unauthorized disclosure of PII, and failed to follow applicable, required, adequate and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party and remained at inappropriate risk of disclosure even before the Data Breach. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

15. Plaintiff Scott Linman is a resident and citizen of the State of Arizona and intends to remain domiciled in and a citizen of the State of Arizona.

16. Defendant Marten Transport, Ltd. is incorporated in the State of Delaware and headquartered at 129 Marten Street, Mondovi, Wisconsin 54755.

17. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

18. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

19. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity.

20. The Western District of Wisconsin has personal jurisdiction over Defendant named in this action because Defendant and/or its parents or affiliates are headquartered in this District and Defendant conduct substantial business in Wisconsin and this District through its headquarters, offices, parents, and affiliates.

21. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

IV. FACTUAL ALLEGATIONS

Background

22. Defendant is a large, publicly traded freight carrier and logistics company with thousands of employees that operates throughout the United States, Canada and Mexico.

23. To apply for jobs with Defendant, Plaintiff and Class Members were required to provide Defendant with sensitive and confidential information, including their names,

dates of birth, and Social Security numbers, which is static information that does not change and can be used to commit a myriad of financial crimes. Applicants must also provide additional information, including, but not limited to, home address history for the past 3 years, current driver license number and driver license history for the last 3 years, and military history (if applicable).[4]

24. Plaintiff and Class Members relied on Defendant (a large, sophisticated entity) to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their PII.

25. Defendant had a duty to take reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties.

26. Defendant has posted a Privacy Policy on its website (the "Privacy Policy"). The Privacy Policy states, in part: "The security for all personally identifiable information associated with guests of the http://www.drive4marten.com Web site is of great concern to Marten Transport Ltd. We exercise caution and great care in providing secure transmission of your information from your PC to our servers."[5]

The Data Breach

27. According to a public filing with the SEC, on October 3, 2021, Defendant "detected a cyberattack that accessed and encrypted files on servers utilized by the

[4] *See* https://intelliapp.driverapponline.com/c/martentransport?r=website-applynow-menu-full&uri_b=ia_martentransport_7209159 (last visited April 5, 2022).
[5] https://www.marten.com/privacy-policy (last visited April 5, 2022).

Company in the provision of its business. The unauthorized access also included the download of certain data files."[6]

28. Defendant has publicly disclosed that the unauthorized actors first gained access to Defendant's system on September 30, 2021. Defendant has further disclosed that despite first discovering the unauthorized access to its systems on October 3, 2021, the unauthorized access to its systems continued until October 4, 2021.

29. Shortly after the Data Breach, a cyber gang called Hive made a post to the dark web claiming responsibility for the attack. In this post, Hive disclosed that it exfiltrated 114 gigabytes of data during the Data Breach.[7]

30. Following the Data Breach, Defendant reports that it began reviewing its records to determine the identities and contact information of victims. Defendant claims it did not complete this review until March 8, 2022, more than five months after the Data Breach.

31. Although Defendant has publicly stated that it began providing notice to "potentially impacted employees" on October 27, 2022, it appears that it did not begin notifying the majority of victims—such as Plaintiff—or state regulators until on or about March 25, 2022.

32. On or about March 25, 2022, Defendant notified various state Attorneys General of the Data Breach. Defendant also provided the Attorneys General with "sample"

[6] https://sec.report/Document/0001437749-21-024381/ (last visited April 4, 2022).
[7] https://mnccservices.com/marten-transport-discloses-cyberattack-warns-employee-data-could-be-at-risk/ (last visited April 4, 2022).

notices of the Data Breach.[8]

33. Defendant admitted in the reports to the Attorneys General and the "sample" notices of the Data Breach that unauthorized third persons "viewed or downloaded" files that contained sensitive information about Defendant's employees and job applicants, including their names and Social Security numbers.

34. Defendant has not shared publicly or with Plaintiff and Class Members, who retain a vested interest in ensuring that their information remains protected, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again.

35. Because of Defendant's actions that allowed for unfettered access to Plaintiff's and Class Members' sensitive information, the unencrypted PII of Plaintiff and Class Members was "viewed or downloaded" and may end up for sale on the dark web, or fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

36. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and Class Members, causing the exposure of PII for approximately 35,294

[8] https://oag.ca.gov/privacy/databreach/list (last visited April 5, 2022); https://apps.web.maine.gov/online/aeviewer/ME/40/386f1029-e915-49dc-bdb6-426bfea19ba2.shtml (last visited April 5, 2022); https://dojmt.gov/consumer/databreach/# (last visited April 5, 2022); https://ago.vermont.gov/blog/2022/03/25/marten-transport-data-breach-notice-to-consumers/ (last visited April 5, 2022); https://www.atg.wa.gov/data-breach-notifications (last visited April 5, 2022).

individuals.

Defendant Acquires, Collects, and Stores the PII of Plaintiff and Class Members.

37. Prior to the Data Breach, Defendant acquired, collected, and stored the PII of Plaintiff and Class Members.

38. As a condition of applying for employment with Defendant, Plaintiff and Class Members entrusted Defendant with highly confidential PII.

39. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

40. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Securing PII and Preventing Breaches

41. Defendant could have prevented this Data Breach by properly securing and encrypting the PII of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data, especially the PII of those who applied for jobs years before the Data Breach.

42. Defendant's policies on its website include promises and legal obligations to take reasonable steps to maintain and protect PII, demonstrating an understanding of the importance of securing PII. For example, "Marten Transport's policy is to respect and protect the privacy of our users…. The security for all personally identifiable information

associated with guests of the http://www.marten.com Web site is of great concern to Marten Transport Ltd. We exercise caution and great care in providing secure transmission of your information from your PC to our servers…. Once we receive your transmission, we make our best effort to ensure its security on our systems."[9]

43. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[10] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[11]

44. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

45. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for

[9] https://www.marten.com/privacy-policy (last visited April 5, 2022).
[10] 17 C.F.R. § 248.201 (2013).
[11] *Id.*

stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[12] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[13] Criminals can also purchase access to entire company data breaches from $900 to $4,500.

46. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[14]

47. It is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and

---

[12] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Jan.17, 2022).
[13] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Jan. 17, 2022).
[14] *Identity Theft and Your Social Security Number*, Social Security Administration, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Jan. 13, 2021).

evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

48. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[15]

49. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, only credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach, including Social Security number and name, is impossible to "close" and difficult, if not impossible, to change—.

50. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained: "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[16]

51. Among other forms of fraud, identity thieves may obtain driver's licenses,

[15] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed Jan. 17, 2022).

[16] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Jan. 17, 2022).

government benefits, medical services, and housing or even give false information to police.

52. The fraudulent activity resulting from the Data Breach may not be fully revealed for years.

53. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[17]

54. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

55. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

---

[17] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last accessed Jan. 17, 2022).

56. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's storage platform, amounting to potentially tens or hundreds of thousands of individuals' detailed, personal information. Thus, there exists a significant number of individuals who would be harmed by the exposure of the unencrypted data.

57. To date, Defendant has offered Plaintiff and Class Members only twelve months of identity theft detection through a single credit bureau, Experian. The offered service is wholly inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

58. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Plaintiff Scott Linman's Experience

59. Plaintiff Scott Linman was required to provide his PII to Defendant when he applied for a job with the Defendant in 2018. Plaintiff Linman was offered a position but did not accept the offer.

60. On or about March 30, 2022, Plaintiff Linman received notice from Defendant that his PII had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Linman's PII, including name and Social Security number, was compromised as a result of the Data Breach. When he applied for the position, Plaintiff Linman gave Defendant additional PII, including his address, date of birth, email, telephone number, financial information, and driver's license number.

61. As a result of the Data Breach, Plaintiff Linman made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; researching and signing up for credit monitoring and identity theft protection services offered by Defendant; and contacting creditors and credit bureaus. Plaintiff Linman has spent approximately two hours dealing with the Data Breach, valuable time Plaintiff Linman otherwise would have spent on other activities, including but not limited to work and/or recreation.

62. As a result of the Data Breach, Plaintiff Linman's debit card information was accessed and used by unauthorized third parties in early March 2022. In a series of fraudulent transactions, the criminals withdrew approximately $140 from his bank account. The bank is still investigating the fraud and has not fully reimbursed Plaintiff Linman for the fraudulent charges. Plaintiff Linman has already spent approximately three hours dealing with the fraudulent charges, valuable time Plaintiff Linman otherwise would have spent on other activities, including but not limited to work and/or recreation.

63. As a result of the Data Breach, Plaintiff Linman has suffered emotional distress as a result of the release of his PII, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PII for purposes of identity theft and fraud. Plaintiff Linman is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

64. Plaintiff Linman suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from Plaintiff Linman; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

65. As a result of the Data Breach, Plaintiff Linman anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Linman is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

V. CLASS ALLEGATIONS

66. Plaintiff brings this nationwide class action on behalf of himself and all others similarly situated under Rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

67. The Nationwide Class that Plaintiff seek to represent is defined as follows:

> **All United States residents whose PII was or could have been accessed during the security incident that is the subject of the notice of data breach that Defendant sent to Plaintiff and other Class Members.**

68. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments,

agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

69. Plaintiff reserves the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

70. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide Class (the "Class") are so numerous that joinder of all members is impracticable. Defendant has identified hundreds of thousands of job applicants whose PII may have been improperly accessed in the Data Breach, and the Class is apparently identifiable within Defendant's records. Defendant advised Maine Attorney General Frey that the Data Breach affected over 35,000 individuals.

71. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendant had duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had duties not to use the PII of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

e. When Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

72. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance.

73. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

74. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages he has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

75. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of

relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

76. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

77. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

78. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

79. Unless a Class-wide injunction is issued, Defendant may continue in its

failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

80. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

81. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiff and Class

Members that their PII had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members; and,

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class)

82. Plaintiff and the Nationwide Class re-allege and incorporate by reference each and every paragraph above as though fully set forth herein.

83. As a condition of applying for jobs with Defendant, Plaintiff and the Nationwide Class were obligated to provide Defendant with certain PII, including their names and Social Security numbers.

84. Plaintiff and the Nationwide Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

85. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Nationwide Class could and would suffer if the PII were

wrongfully disclosed.

86. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiff and the Nationwide Class involved an unreasonable risk of harm to Plaintiff and the Nationwide Class.

87. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, configuring, maintaining, and testing Defendant's security protocols to ensure that the PII of Plaintiff and the Nationwide Class in Defendant's possession was adequately secured and protected.

88. Defendant also had a duty to exercise appropriate clearinghouse practices to remove job applicants' PII it was no longer required to retain pursuant to regulations.

89. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiff and the Nationwide Class.

90. Defendant's duty to use reasonable security measures arose as a result of the relationship that existed between Defendant and Plaintiff and the Nationwide Class. That relationship arose (95because Plaintiff and the Nationwide Class entrusted Defendant with their confidential PII, a necessary part of applying for jobs with Defendant.

91. Defendant was subject to an independent duty untethered to any contract between Defendant and Plaintiff or Defendant and the Nationwide Class.

92. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Nationwide Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

93. Plaintiff and the Nationwide Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Nationwide Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII.

94. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Nationwide Class. Defendant's misconduct included, but was not limited to, its failure to encrypt the data stored on its system or to implement other reasonable industry standard measures to safeguard PII.

95. Plaintiff and the Nationwide Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

96. Defendant was in a position to protect against the harm suffered by Plaintiff and the Nationwide Class as a result of the Data Breach.

97. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Nationwide Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Nationwide Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

98. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and the Nationwide Class.

99. Defendant has admitted that the PII of Plaintiff and the Nationwide Class

was exposed to unauthorized third persons as a result of the Data Breach.

100. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Nationwide Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and the Nationwide Class during the time the PII was within Defendant's possession or control.

101. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

102. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiff and the Nationwide Class in the face of increased risk of theft.

103. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Nationwide Class by failing to have appropriate procedures in place to detect and prevent dissemination of job applicants' PII.

104. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove job applicants' PII it was no longer required to retain pursuant to regulations.

105. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Nationwide Class the existence and scope of the Data Breach.

106. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, the PII of Plaintiff and the Nationwide Class would not

have been compromised.

107. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The PII of Plaintiff and the Nationwide Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

108. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

109. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it collected and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Nationwide Class.

110. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

111. Plaintiff and the Nationwide Class are within the class of persons that the FTC Act was intended to protect.

112. The harm that occurred as a result of the Data Breach is the type of harm the

FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Nationwide Class.

113. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiff and the Nationwide Class; and (viii) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Nationwide Class.

114. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Nationwide Class have suffered and will continue to suffer other

forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

115. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Nationwide Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

116. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Nationwide Class are entitled to recover actual, consequential, and nominal damages.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Nationwide Class)

117. Plaintiff and the Nationwide Class re-allege and incorporate by reference each and every paragraph above as though fully set forth herein.

118. Defendant required Plaintiff and the Nationwide Class to provide their personal information, including names and Social Security numbers, as a condition of applying for employment.

119. As a condition of applying for employment with Defendant, Plaintiff and the Nationwide Class provided their personal information. In so doing, Plaintiff and the Nationwide Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and

confidential, and to timely and accurately notify Plaintiff and the Nationwide Class if their data had been breached and compromised or stolen.

120. Plaintiff and the Nationwide Class fully performed their obligations under the implied contracts with Defendant.

121. Defendant breached the implied contracts it made with Plaintiff and the Nationwide Class by (i) failing to implement technical, administrative, and physical security measures to protect the PII from unauthorized access or disclosure and improper (such as encryption of Social Security numbers) despite such measures being readily available, (ii) failing to limit access to the PII to Defendant's employees who needed such ass to perform a specific job, (iii) failing to store the PII only on servers kept in a secure, restricted access area, and (iv) otherwise failing to safeguard the PII.

122. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Nationwide Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

123. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Nationwide Class are entitled to recover actual, consequential, and nominal damages.

COUNT III
INVASION OF PRIVACY
(On Behalf of Plaintiff and the Nationwide Class)

124. Plaintiff and the Nationwide Class re-allege and incorporate by reference each and every paragraph above as though fully set forth herein.

125. Plaintiff and the Nationwide Class had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

126. Defendant owed a duty to its prospective, current, and former employees, including Plaintiff and the Nationwide Class, to keep their PII contained as a part thereof, confidential.

Defendant failed to protect and released to unknown and unauthorized third partiesthe PII of Plaintiff and the Nationwide Class.

127. Defendant allowed unauthorized and unknown third parties access to and examination of the PII of Plaintiff and the Nationwide Class, by way of Defendant's failure to encrypt, secure, or delete the PII. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiff and the Nationwide Class is highly offensive to a reasonable person.

128. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and the Nationwide Class disclosed their PII to Defendant as part of

their prospective, current, and former employment with Defendant, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and the Nationwide Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

129. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff's and the Nationwide Class' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

130. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it had actual knowledge that its information security practices were inadequate and insufficient.

131. Because Defendant acted with this knowing state of mind, they had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the Nationwide Class.

132. As a proximate result of the above acts and omissions of Defendant, the PII of Plaintiff and the Nationwide Class was disclosed to third parties without authorization, causing Plaintiff and the Nationwide Class to suffer damages.

133. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Nationwide Class in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come, Plaintiff and Class Members have no

adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and Class Members.

COUNT IV
BREACH OF CONFIDENCE
(On Behalf of Plaintiff and the Nationwide Class)

134. Plaintiff and the Nationwide Class re-allege and incorporate by reference each and every paragraph above as though fully set forth herein.

135. At all times during Plaintiff's and the Nationwide Class's interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and the Class Members' PII that Plaintiff and Class Members provided to Defendant.

136. As alleged herein and above, Defendant's relationship with Plaintiff and the Nationwide Class was governed by terms and expectations that Plaintiff's and the Nationwide Class's PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

137. Plaintiff and the Nationwide Class provided their PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII to be disseminated to any unauthorized third parties.

138. Plaintiff and the Nationwide Class also provided their PII to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that PII from unauthorized disclosure.

Defendant voluntarily received in confidence Plaintiff's and Class Members' PII with the understanding that PII would not be disclosed or disseminated to the public or any unauthorized third parties.

139. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiff's and Class Members' PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

140. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and the Nationwide Class have suffered damages.

141. But for Defendant's disclosure of Plaintiff's and the Nationwide Class's PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' PII as well as the resulting damages.

142. The injury and harm Plaintiff and the Nationwide Class suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' PII. Defendant knew or should have known its methods of accepting and securing PII was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiff's and Class Members' PII.

143. As a direct and proximate result of Defendant's breach of its confidence with Plaintiff and the Nationwide Class, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery

from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of prospective, current, and former employees; and (viii) present and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

144. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT V
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Nationwide Class)

145. Plaintiff and the Nationwide Class re-allege and incorporate by reference each and every paragraph above as though fully set forth herein.

146. Defendant benefited from receiving Plaintiff's and Class Members' PII by its ability to retain and use that information for its own benefit. Defendant understood this benefit.

147. Defendant also understood and appreciated that Plaintiff's and Class Members' PII was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

148. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the form of providing an ability to find people to employ, and in connection thereto, by providing their PII to Defendant with the understanding that Defendant would pay for the administrative costs of reasonable data privacy and security practices and procedures. Specifically, they were required to provide Defendant with their PII. In exchange, Plaintiff and Class Members should have received adequate protection and data security for such PII held by Defendant.

149. Defendant knew Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

150. Defendant failed to provide reasonable security, safeguards, and protections to the PII of Plaintiff and Class Members.

151. Under the principles of equity and good conscience, Defendant should not be permitted to retain money belonging to Plaintiff and Class members, because Defendant failed to implement appropriate data management and security measures mandated by industry standards.

152. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class Members.

153. Defendant's enrichment at the expense of Plaintiff and Class Members is and was unjust.

154. As a result of Defendant's wrongful conduct, as alleged above, Plaintiff and Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class and appointing Plaintiff and his Counsel to represent such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local

laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating

firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to

appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Respectfully Submitted,

HELLMUTH & JOHNSON PLLC

/s/ *Anne T. Regan*
Anne T. Regan
Nathan D. Prosser*
8050 West 78th Street
Edina, MN 55439
Phone: (952) 941-4005
Fax: (952) 941-2337
aregan@hjlawfirm.com
nprosser@hjlawfirm.com

M. Anderson Berry*
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Facsimile: (916) 924-1829
aberry@justice4you.com

Terence R. Coates*
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, OH 45202
Telephone: (513) 651-3700
Facsimile: (513) 665-0219
tcoates@msdlegal.com

Attorneys for Plaintiff and the Proposed Class

**pro hac vice forthcoming*